

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平10-40095

(43)公開日 平成10年(1998)2月13日

(51)Int.Cl. ⁴	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 A
A 6 3 F 7/02	3 3 4		A 6 3 F 7/02	3 3 4
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B

審査請求 未請求 請求項の数3 OL (全 8 頁)

(21)出願番号 特願平8-198182

(22)出願日 平成8年(1996)7月26日

(71)出願人 591107481

株式会社エルイーテック

東京都千代田区一ツ橋2丁目6番3号

(72)発明者 今井 信正

東京都千代田区一ツ橋2丁目6番3号 株

式会社エルイーテック内

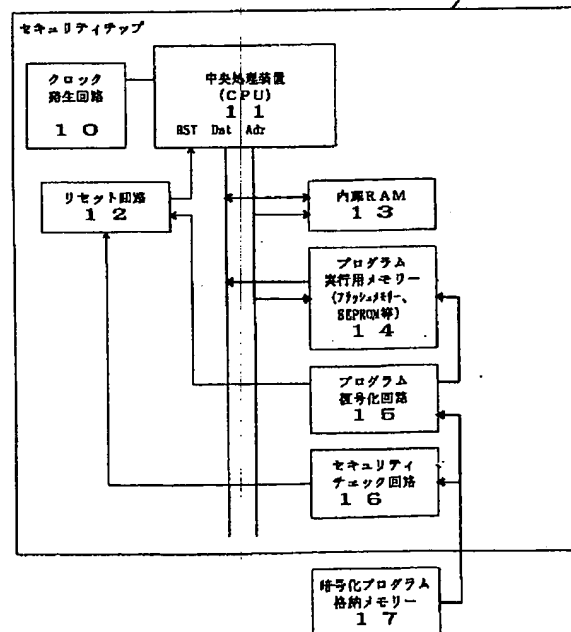
(74)代理人 弁理士 稲木 次之 (外1名)

(54)【発明の名称】 プログラム実行メモリー内蔵のセキュリティチップ

(57)【要約】 (修正有)

【課題】 制御基板に搭載するチップの認定後に、プログラムを格納するためのメモリーを二重化する事により不正行為を防止するセキュリティチップを提供する。

【解決手段】 クロック発生回路10、中央処理装置11、内蔵RAM13、リセット回路12、プログラム実行メモリー14、暗号化プログラム格納メモリー17、プログラム復号化回路15、セキュリティチェック回路16で構成する。暗号化プログラムのセキュリティチェックの後に、復号したユーザプログラム(UP)もチェックを行い、正規の場合のみプログラムに従い制御する。また、暗号化して格納するメモリーをチップとは別のメモリーで構成する。



【特許請求の範囲】

【請求項1】 クロック発生回路と接続された中央処理装置（CPU）と、該CPUとバスを介して接続された内蔵RAM及びプログラム実行用のフラッシュメモリ、EEPROM等のメモリと、前記CPUのリセット部と接続されたリセット回路と、認証されたユーザープログラム（UP）を暗号化した状態で格納するためのメモリと、該格納メモリに記憶された暗号化ユーザープログラム（UP'）を読み込む際にセキュリティチェックを行うセキュリティチェック回路と、前記セキュリティチェック回路において正規と確認された場合に暗号化ユーザープログラム（UP'）を復号化するプログラム復号化回路と、該プログラム復号化回路で復号化されたプログラムを遊技機制御のために格納するプログラム実行用のメモリとからなり、正規の場合のみ前記プログラム実行用のメモリに格納されたプログラムに従い制御するように構成されていることを特徴とするプログラム実行メモリ内蔵のセキュリティチップ。

【請求項2】 クロック発生回路と接続された中央処理装置（CPU）と、該CPUとバスを介して接続された内蔵RAM及びプログラム実行用のフラッシュメモリ、EEPROM等のメモリと、前記CPUのリセット部と接続されたリセット回路と、認証されたユーザープログラム（UP）を暗号化した状態で格納するためのメモリと、該格納メモリに記憶された暗号化ユーザープログラム（UP'）を読み込む際にセキュリティチェックを行うセキュリティチェック回路と、前記セキュリティチェック回路において正規と確認された場合に暗号化ユーザープログラム（UP'）を復号化するプログラム復号化回路と、該プログラム復号化回路で復号化されたプログラムを遊技機制御のために格納するプログラム実行用のメモリとからなり、暗号化プログラムのセキュリティチェックの後に前記プログラム復号化回路において復号化されたユーザープログラム（UP）についてもセキュリティチェックを行い、復号化の前後におけるユーザープログラム（UP）のセキュリティチェックで正規の場合のみ前記プログラム実行用のメモリに格納されたプログラムに従い制御するように構成されていることを特徴とするプログラム実行メモリ内蔵のセキュリティチップ。

【請求項3】 前記認証されたユーザープログラム（UP）を暗号化した状態で格納するためのメモリがチップとは別のメモリで構成したことを特徴とする請求項1又は請求項2記載のプログラム実行メモリ内蔵のセキュリティチップ。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、パチンコ、回胴式等の遊技機の制御基板に搭載される第三者認定機関において検査を受けたプログラムが組み込まれたマイクロ

ンピュータチップ（以下チップという）において、当該認定プログラムが改変されないようにするためのチップに関するものである。

【0002】

【従来技術】 従来のチップでは、認定されたプログラムが格納されたメモリに基づき遊技機を制御する遊技機の電源投入当初において、当該メモリにキーコードと共に格納されたプログラムが正規のものであるか否についてチップに搭載されたセキュリティ回路が、認証コードの整合性に関するセキュリティチェックを行い、チェックの結果正規と認定された場合に制御プログラムの作動を認め、メモリに格納されたプログラムに基づき遊技機を制御させるように構成されたものが発明されている（特開平03-118120号）。

【0003】

【発明が解決しようとする課題】 かかる従来のチップでは、メモリを認定を受けた正規のものから不正のものに取り替えたり、認定後に内部のプログラムを改変した場合に、不正行為を発見し遊技機の作動を認めないようにすることができる。しかしながら、かかるチップのセキュリティ回路は、遊技機の電源立ち上げ時にセキュリティ回路が始動するように構成されているために一端起動した後は、セキュリティチェックが行われないために、次のような不正行為が行われる可能性を有している。すなわち、正規のプログラムが格納されたメモリと並列に不正プログラムが格納された不正メモリを装着しておき、チップによるセキュリティチェックが行われる時には、正規のプログラムが格納されたメモリを接続し、セキュリティチェック終了後に不正メモリの方に切り替えて不正メモリに格納されたプログラムに基づき制御する二重化ROM方式による不正が考えられる。そこで、かかる不正行為をも防止することができる安全なチップを提供することを目的とする。

【0004】

【課題を解決するための手段】 すなわち本発明は、クロック発生回路と接続された中央処理装置（CPU）と、該CPUとバスを介して接続された内蔵RAM及びプログラム実行用のフラッシュメモリ、EEPROM等のメモリと、前記CPUのリセット部と接続されたリセット回路と、認証されたユーザープログラム（UP）を暗号化した状態で格納するためのメモリと、該格納メモリに記憶された暗号化ユーザープログラム（UP'）を読み込む際にセキュリティチェックを行うセキュリティチェック回路と、前記セキュリティチェック回路において正規と確認された場合に暗号化ユーザープログラム（UP'）を復号化するプログラム復号化回路と、該プログラム復号化回路で復号化されたプログラムを遊技機制御のために格納するプログラム実行用のメモリとからなり、正規の場合のみ前記プログラム実行用のメモリに格納されたユーザープログラムに従い制御

するように構成されたプログラム実行メモリ内蔵のセキュリティチップ。請求項2の発明は、前記構成のチップにおいて暗号化プログラムのセキュリティチェックの後に前記プログラム復号化回路において復号化されたユーザープログラム(UP)についてもセキュリティチェックを行い、復号化の前後におけるユーザープログラム(UP)のセキュリティチェックで正規の場合のみ前記プログラム実行用のメモリに格納されたプログラムに従い制御するように構成されたプログラム実行メモリ内蔵のセキュリティチップ。請求項3の発明は、前記認証されたユーザープログラム(UP)を暗号化した状態で格納するためのメモリをチップとは別の外付けメモリで構成したものである。

【0005】

【作用】本発明にかかるセキュリティチップでは、予め認定ユーザープログラム(UP)とセキュリティコード(K1)を暗号化し、これら暗号化データと該暗号化データについてセキュリティチェックするためのセキュリティコード(K2)を暗号化プログラム格納メモリに格納しておき、遊技機の電源投入当初はこの暗号化プログラム格納メモリに格納された暗号化ユーザープログラム(UP')及び該暗号化プログラムのセキュリティコード(K1')からなるデータをセキュリティコード(K2)に基づきプログラムが正規のものか否かについてセキュリティチェックを行い、チェックの結果異常の場合にはリセット回路を介して遊技機の作動を制止する。またセキュリティチェックの結果正規と判断された場合には、暗号化プログラム格納メモリに格納された暗号化ユーザープログラム(UP')及び該暗号化プログラムのセキュリティコード(K1')がプログラム復号化回路に送られ、そこで復号化処理が行われ、第三者検査機関で検定を受けたユーザープログラム(UP)としてプログラム実行用メモリにインストールされる。制御基板においては、当該プログラム実行用メモリにインストールされたユーザープログラム(UP)に基づき内蔵RAMを使用しながら遊技機を制御することになる。

【0006】また請求項2の発明では、前記セキュリティチェック回路において暗号化ユーザープログラム(UP')及び該暗号化セキュリティコード(K1')をセキュリティコード(K2)に基づきプログラムが正規のものか否かについてセキュリティチェックを行った後にプログラム復号化回路において暗号を復号化したものをプログラム実行用メモリにインストールした後に復号化されたユーザープログラム(UP)をセキュリティコード(K1)に基づきセキュリティチェック回路において再度セキュリティチェックを行い、その結果プログラムが正規と判定されなかった場合には、リセット回路を介して遊技機の作動を制止する。また正規と判定された場合には、当該プログラム実行用メモリにインスト

ールされたプログラムに基づき内蔵RAMを使用しながら遊技機を制御することになる。

【0007】尚、データを暗号化(エンクリプション)する方法としては、キーコード(鍵)を設定し、これをアメリカのDES(Data encryption Standard)又は日本電信電話株式会社のFEAL8(Fast data Encipherment Algorithm)等の規格を用いて暗号化・復号化する方法が考えられる。

【0008】

【発明の実施の形態】以下に本発明を図示された実施例に従って詳細に説明する。図1において1は、遊技機の制御基板に搭載されるマイクロコンピュータチップ(以下チップという)であり、該チップ1はクロック発生回路10の発生するクロック信号に基づきデータの受け入れを行う中央処理装置(CPU)11と、該CPU11の内部データベース及びアドレスバスを介して接続されたユーザーアプリケーションプログラムのワークRAM13及びユーザーのアプリケーションプログラムをインストールするためのプログラム実行用のフラッシュメモリ、EEPROM等のメモリ14と、所定のキーコード(鍵)に基づき暗号化されたデータを復号化するプログラム復号化回路15と、第三者検査機関において検査を受けたユーザーアプリケーションプログラムを所定のキーコードに基づき暗号化されたものを格納する暗号化プログラム格納メモリ17のデータを所定のセキュリティコード(K2)に基づきセキュリティチェックを行うセキュリティチェック回路16と、該セキュリティチェック回路16からの送信信号に基づき、CPU11をリセットするリセット回路12とからなり、前記プログラム復号化回路15とリセット回路12及びプログラム実行用メモリ14とが接続されている。

【0009】次に図2に示すものは本発明の第2実施例を示すもので、前記第1実施例のチップにおいて、プログラム実行用メモリ14に格納されたユーザープログラム(UP)を所定のセキュリティコード(K1)に基づきセキュリティ回路16でセキュリティチェックするような構成としたものである。

【0010】図3に示すものは本発明の第3実施例を示すもので、前記暗号化プログラム内蔵メモリ37をチップ1に内蔵させ、第三者検査機関で検定を受けた正規のプログラムをセキュリティコード(K1)と共に書き込み回路38を介して暗号化した状態で格納するように構成したものであり、他の構成は前記第2実施例と同じであるので符号番号を同一にして説明を省略する。

【0011】以上述べた構成において、本実施例にかかるチップでは、図4に示すようにユーザーが開発した遊技機のプログラム(以下ユーザープログラム(UP)という)に関して第三者検査機関により検定を受けた後に該ユーザープログラム(UP)を元に算出されたセキュリティコードが付与される。このユーザープログラム

(UP) 及びセキュリティコード(K1)が所定のキーコード(鍵)に基づき暗号化されて、該暗号化データのセキュリティコード(K2)と共に暗号化プログラム格納メモリ17にインストールされる。実施例3の内蔵メモリ37へは書き込み回路38を介して暗号化されたユーザープログラム(UP')及びセキュリティコード(K1')と暗号化のためのセキュリティコード(K2)がインストールされる。以上により制御基板のチップの状態となる。

【0012】かかる状態においてチップの電源を投入するとまずセキュリティチェック回路16はセキュリティコード(K2)に基づき各アドレスのデータを走査することによりセキュリティチェックを行う。セキュリティチェックの結果データに誤りを発見した時には、リセット回路12に対してリセット命令が発信され、CPU11の作動を停止する。一方データが正しいと判断した時には、暗号化されたユーザープログラム(UP')及びセキュリティコード(K1')をプログラム復号化回路15に送り所定の暗号化コード(鍵)に基づき各アドレスのデータを復号化させ、復号化されたユーザープログラム(UP)及びセキュリティコード(K1)をチップ1内部のプログラム実行用メモリ14にインストールを行う。そして第1実施例のチップでは、CPU11はプログラム実行用メモリ14に格納されたユーザープログラム(UP)を読み込みながら遊技機を制御することになる。

【0013】また前記第2及び第3実施例のチップ1では、プログラム実行用メモリ14に格納されたユーザープログラム(UP)及びセキュリティコード(K1)に基づき再度セキュリティチェック回路16にセキュリティチェックを行わせ、復号化したプログラムが正規のものである否かについて判断させる。その結果ユーザープログラム(UP)のセキュリティチェックにおいてデータが一致しなかった時には、メモリ14に格納されたユーザープログラム(UP)は正規のものではないと判断して、リセット回路12にCPU11をリセットさせて遊技機の作動を制止させる。またセキュリティチェックにおいてデータが整合した場合には、プログラムが正規のものであると判断し、CPU11はワークRAM13にプログラムを読み込みながら遊技機を制御する。

【0014】以上述べたように本発明にかかるマイクロコンピュータチップでは、暗号化されたユーザープログラム(UP')を復号化することにより該プログラムを

内部メモリにインストールして作動するように構成しているので二重化ROMを切り替え使用するような不正行為を防止することができる。また本発明にかかるチップでは第三者検査機関において認定されたプログラムを所定のキーコードに基づき暗号化した状態でメモリにインストールしているので、開発者以外の者が容易にプログラムの解析を行うというような行為を未然に防ぐことができる。さらに、チップ内蔵のプログラム実行用メモリにユーザープログラム(UP)をインストールさせてから遊技機の制御を行うように構成しているので、内部バス等の高速・安定な回路を介して情報のやりとりを行うことになるので、ノイズの影響や誤動作を発生を極力防ぐことができる。さらにまた、暗号化ユーザープログラム(UP')と復号化プログラム(UP)の双方について、セキュリティチェックを行うように構成したものである、暗号化方法をクリアしてプログラムを改変しても復号化プログラム(UP)のセキュリティチェックにおいて正規のもの否かが判定されることとなるために、双方のセキュリティチェックをパスするような状態でプログラムを改変することは実質的に不可能な状態となる。

【図面の簡単な説明】

【図1】 本発明にかかるマイクロコンピュータチップの第1実施例を示すブロック図である。

【図2】 本発明にかかるマイクロコンピュータチップの第2実施例を示すブロック図である。

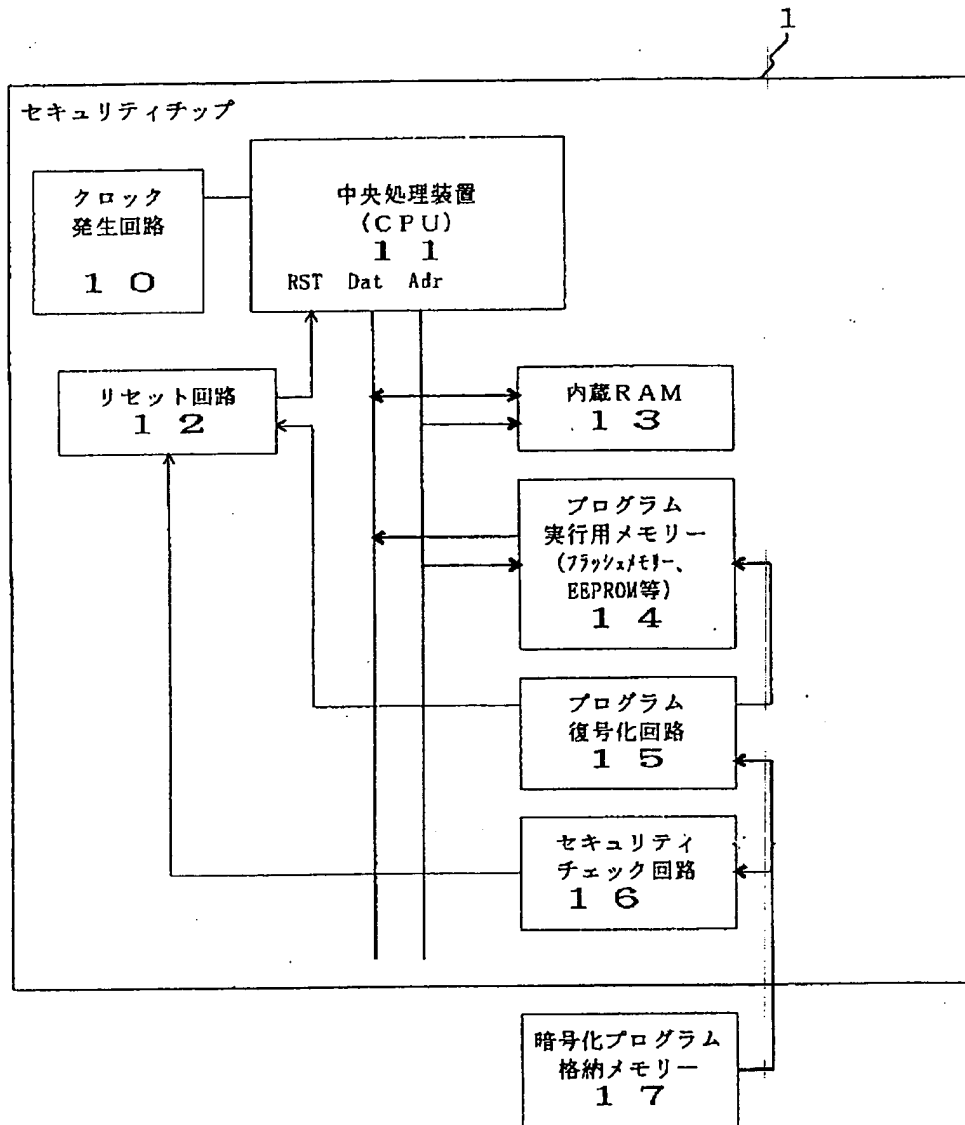
【図3】 本発明にかかるマイクロコンピュータチップの第3実施例を示すブロック図である。

【図4】 第三者検査機関において認定を受けたユーザープログラム(UP)のメモリ、暗号化プログラム格納メモリ及びプログラム実行用メモリに格納されたデータの状態を示す概念図である。

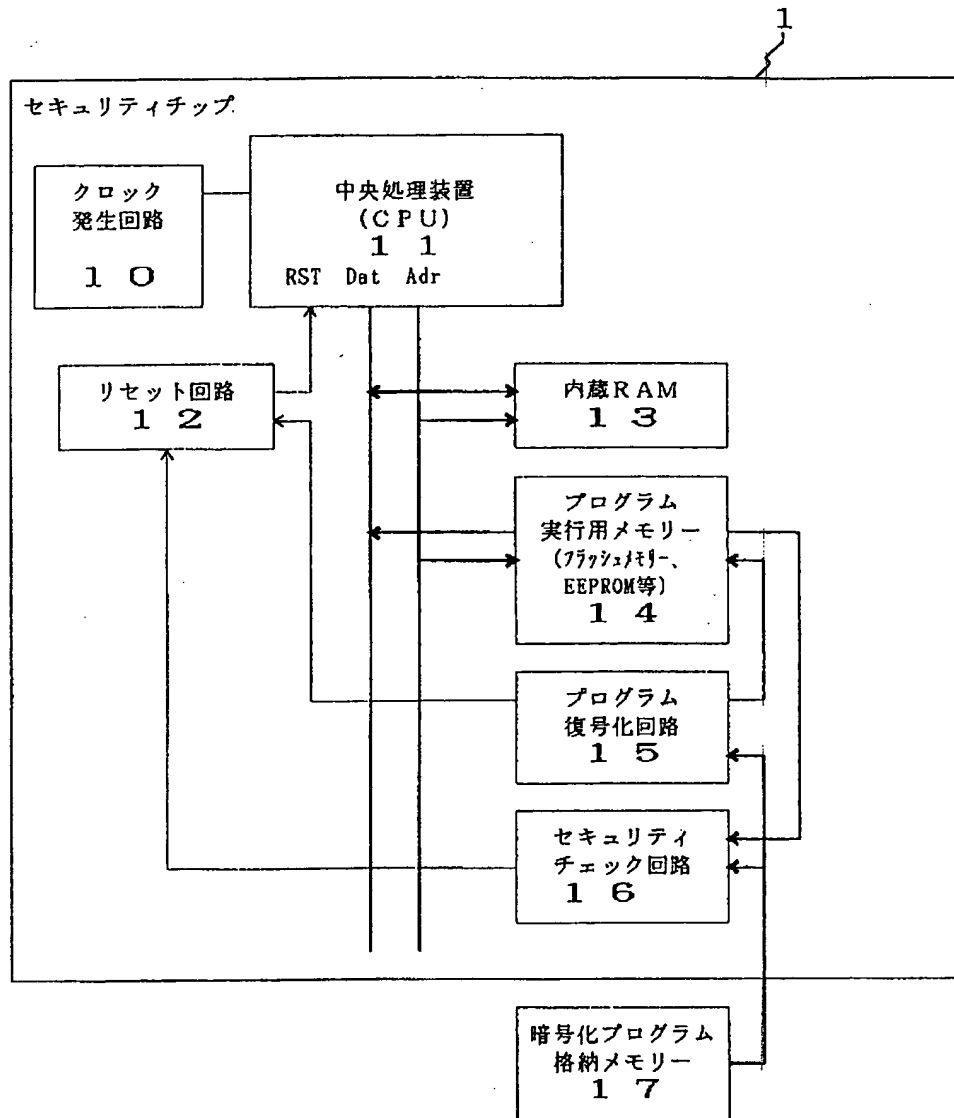
【符号の説明】

1	チップ
10	クロック発生回路
11	CPU
12	リセット回路
13	内蔵RAM
14	プログラム実行用メモリ
15	プログラム復号化回路
16	セキュリティチェック回路
17, 37	暗号化プログラム格納メモリ
38	書き込み回路

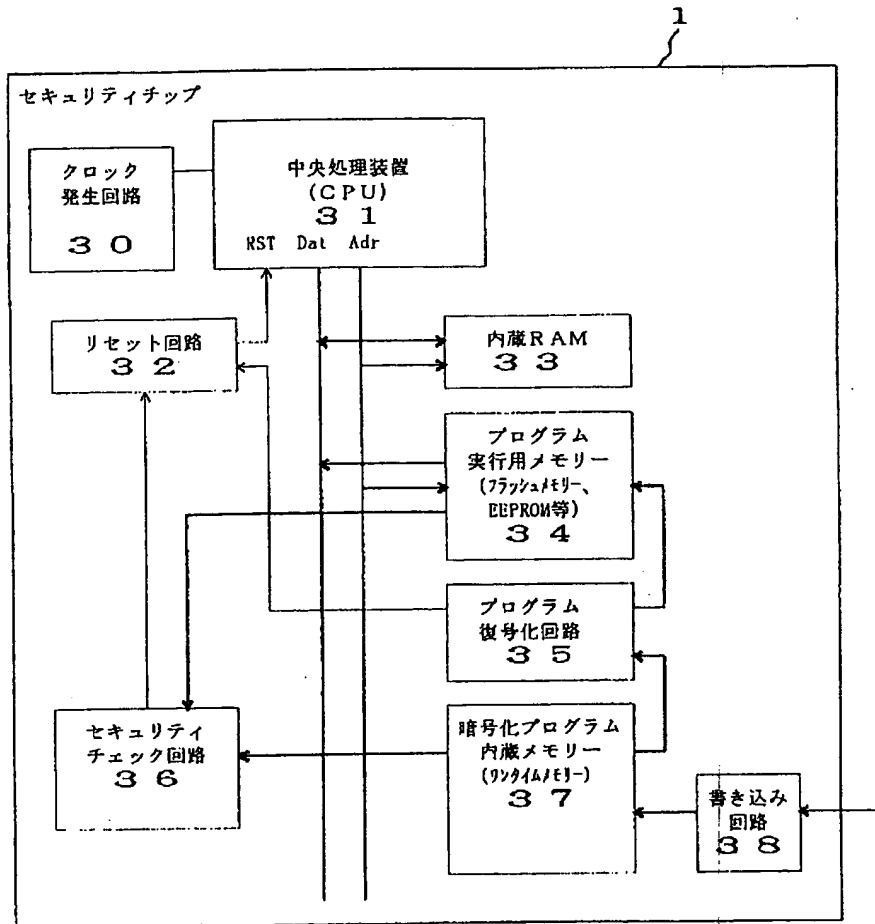
【図1】



【図2】



【図3】



【図4】

